



Tuesday, 28th February 2023

**2023-2030 Cyber Security Strategy Discussion Paper
Expert Advisory Board**
Australian Government
Canberra ACT 2600

Via email submission to: auscyberstrategy@homeaffairs.gov.au

PUBLIC SUBMISSION

I write to make this public submission as part of the Australian Government's *2023-2030 Cyber Security Strategy Discussion Paper* with public submissions and feedback sought until 15th April 2023.

I acknowledge the appointment of the Expert Advisory Board members, Chaired by Mr Andrew Penn AO, Mel Hupfeld AO DSC and Rachael Falk.

I too would like to see Australia become a world-leader in cyber security by 2030 and I acknowledge the Australian Government's detailed discussion paper and comprehensive commitment in this area of cyber security policy reform.

I would like to submit the following seven key policy recommendations for consideration as part of this cyber strategy discussion paper and public consultation process:

1. That the Australian Government re-doubles its efforts to enable a strong sovereign capability to help to counteract any cyber security risks or threats to Australians.
2. That the Australia Government increases its 2023-2024 Federal Budget funding allocation, lifts its allocation of resources and support for both regulators, law enforcement agencies and also the Australian Cyber Security Centre, who are our preeminent cyber intelligence agency in Australia to help ensure that they have the trained staff needed and the adequate resources needed to help to better identify and to mitigate risks and potential cyber security threats to Australia.
3. That the Australian Government embraces a nationally coordinated approach to cyber security that responds to new realities, reduces vulnerabilities, deters adversaries, and safeguards opportunities for the Australian people to thrive and prosper through until 2030 and beyond.
4. That the Australian Government fosters and protects Australian invention and innovation which is critical – to nurture innovation by promoting institutions and programs

that drive our competitiveness and counter predatory mergers and acquisitions and counter intellectual property theft.

5. That the Australian Government supports the growth of future innovation and technologies, which include artificial intelligence, quantum information science, and next-generation telecommunication infrastructure.
6. That the Australian Government commits to expanding our international influence abroad via diplomatic efforts with our partners in the region to extend the key tenets of an open, interoperable, reliable and secure Internet.
7. That the Australian Government develops a new *Cyber Security Strategy Guide and Best Practice Handbook* to all Commonwealth Government staff, departments and Commonwealth agencies to ensure that senior public servants in each Commonwealth department and agency are taking proactive leadership and implementing internal cyber security procedures with other public servants based on evidence and best practice. It could also include useful, practical information on how to effectively identify, report and manage any potential cyber risks or online threats.

Thank you very much for the opportunity to make a small contribution with this public submission as part of the Australian Government's 2023-2030 Cyber Security Strategy discussion paper consultation process.

I hope that many other Australians including leaders in business and industry and the various experts involved in mitigating cyber security risks also make a contribution in the coming days and weeks on a wide range of discussion points.

Mr Ben Blackburn
Managing Director
Ben Blackburn Racing